Exhibit A

KROLL

Kroll Acceptable Use of Assets Policy

Last Updated October 2023

TABLE OF CONTENTS

1 Introduction

Kroll and its associated companies (collectively "the Firm" are committed to protecting confidential and sensitive Firm and client information("Information"). This Acceptable Use of Assets Policy (hereinafter, the "Policy")) is designed to protect the Firm, its employees, and clients from prohibited, damaging, unauthorized or other illegal actions that may jeopardize the security, integrity and confidentiality of Information and Firm Information Technology ("IT") systems. It is the responsibility of everyone associated with the Firm to maintain and protect Information.

2 Scope

This Policy applies to all Firm employees, independent contractors, consultants, suppliers / vendors and any other user of the Firm's systems or computing resources. All are required to adhere to established requirements within this Policy when using Firm assets, computer equipment and/or the Firm network.

All aspects of this Policy, including compliance, Firm rights (including monitoring) and enforcement, are to be performed in accordance with local, state, federal and international laws, and restrictions. If specific sections, requirements, or Firm rights contained in this Policy are determined as not applicable or not enforceable under local law, all other sections and requirements remain in place.

3 Description

All Firm resources and all information transmitted by, received from, or stored in these systems are the property of the Firm (and/or its clients or software/service providers) and, as such, are provided for official Firm business. Access to these resources is governed by the Access Control Policy. All messages or information composed, sent, received, or stored using the Firm-provided email system, instant messaging tools, network, internet, intranet or any other Firm-provided or approved system or service are and shall remain the property of the Firm, including passwords.

Unless specifically called for by law, none of the items mentioned herein shall be the private or personal property of any individual, and individuals should not have an expectation of privacy for any messages or communications transmitted via Firm-provided electronic resources. Firm systems are to be used to conduct Firm business. However, the Firm allows use of its systems for incidental and occasional personal use. Limited non-business use of Firm system must be reasonable and respectful and may not interfere with conducting Firm business or violate Firm policies or applicable law. This incidental use should be temporary and shall not include storage of personal files. The Firm is not required to return any personal content to an individual during employment or when they leave the Firm. If an exception is made, the Information Security Team will be the sole approver and will decide on the method of transfer.

Employees shall not to use Firm systems for personal banking, investments, or medical management. This type of data contains personal information that could be discoverable in a court proceeding and may be subject to monitoring as part of Kroll's routine internet monitoring protocol.

4 Policy Exceptions Requests

Any exceptions to this policy must be reviewed and approved by Chief Information Security Officer/Deputy Chief Information Security Officer (CISO/DCISO).

5 Policy Violations

Violations of this Policy may result in corrective or adverse action, up to and including termination of employment or other appropriate action in the case of non-employees.

6 General Acceptable Use

Notwithstanding the Firm's right to retrieve and read any message or information on Firm-provided wireless devices (e.g., text messages), email, internet, intranet or any other Firm-provided or approved system or service, such messages or information should be treated as confidential by others and accessed only by the intended recipient. Except for those working in information security, fraud detection/prevention, investigative, legal, compliance or human capital roles when they are acting in furtherance of their official duties, no one is authorized to retrieve or read any message or information that is not sent to them, nor should they attempt to gain access to another's messages or information.

Users are responsible for ensuring their use of a Firm's IT resource is appropriate given this Policy. If the appropriate use of an IT resource is unclear, the user must consult with his or her supervisor or manager and/or the Firm's IT department to establish whether the use is appropriate ***prior to*** using the resource in that manner.

- The Firm supplies equipment to those whose work requires access to the Firm resources. This equipment and its configuration must not be modified outside of the approved processes.
- The use of personal devices to connect to Firm network resources other than by use of the approved Virtual Desktop Infrastructure (VDI) solution is strictly prohibited. When using the VDI solution for remote connectivity no data should be printed, photographed, or copied from the VDI to the personal device.
    - Firm-owned or licensed software is to be installed only on Firm-managed devices.
    - VPN access to Firm network assets is prohibited from any non- Firm- managed device.

- Users must not attempt to connect any device, including but not limited to computers, networking equipment, storage devices, “Internet of Things” (IoT) devices, etc. to the network without prior approval from Information Security.
- Users are responsible for protecting Firm IT resources assigned to them or to which they have access (including, but not limited to, physical devices, user identities and email messages).
    - Physical devices (i.e., laptops, mobile phones, tablets, portable storage media and other mobile devices) must be securely safeguarded when they are not in use.
    - Lost, misplaced, or stolen Firm IT resources must be reported immediately to the One Point/ Service Desk or appropriate department.
    - Users must lock their screen whenever they leave a computing device unattended. Firm systems have features designed to prohibit access by others when not in use (e.g., screensavers with password protection). Such features are to be always active.
    - Computers, laptops, mobile phones, and other Firm electronic devices are not to be left unattended at any time unless secured in a secure location, such as, a hotel safe. Any device that is left must be left in a switched off state (not sleep).
    - All access devices will be returned to the Information Technology Team when the employee is on vacation or long-term Leave of Absence that lasts for more than 40 consecutive days. The Information Security Management Team will be the sole source of approval for any exceptions.
    - Confidential/restricted/internal data cannot be stored on portable devices/media unless:
        - Authorized by the Information Security, Legal and Compliance departments.
        - Such storage is not in violation of regulatory or contractual obligations.
        - Utilized for information transfer only and not long term or permanent storage.
        - Appropriate controls are put in place to safeguard the data such as encryption.
- Firm resources are to be utilized in a professional, ethical, and lawful manner always.
- Authentication information, such as, usernames, passwords, and PINs must not be documented and carried with any portable devices or media, unless encrypted in a manner approved by the CIO and CISO. This includes saving passwords, scripting logins, or creating macros capable of automatically entering credentials.

- Employees, independent contractors, and consultants are prohibited from using third-party software, file sharing solutions or email providers (e.g., Gmail, MSN, Hotmail, etc.) to create, send, receive, or store Firm information. Exception requests must be submitted to one point/Service Desk and will be reviewed appropriately by Information Security. Review criteria will include:
    - Valid business justification
    - Benefit to the Firm
    - Availability of more secure options
    - Risk to the Firm

  Exceptions may be granted if a client instructs the use of an external file sharing service controlled or managed by that client.
- Use of client or regulatory body messaging services (e.g., chat services) requires the approval of Information Security, and in certain cases, Compliance/Privacy/Legal depending on the request.
- Users of Firm IT resources should not have any expectation of privacy in connection with the use of resources or with the transmission, receipt or storage of messages or information utilizing these resources.
- All information contained in email and other messages to and from the Firm's systems could be subject to legal discovery and other review. It is critical to treat email as formal business communications rather than informal conversations.
- When using email, users are expected to comply with the normal standards of professional and personal courtesy and conduct.
- Do not use the Firm's email system and IT resources for personal mass mailings, third-party commercial activity, political campaigning, and the pursuit of charitable donations or the dissemination of chain letters.
- Users shall not use corporate email addresses for anything that is not directly related to work. This includes personal file share sites, social media, personal communications platforms, entertainment, personal financial sites, and medical plans. All data that is associated with the firm's corporate email addresses is the property of Kroll.
- Do not transmit sensitive personal information or confidential or other sensitive employee/client information in clear text. *(Users needing to send this type of Information to internal or external recipients must use some form of encryption (i.e., PGP, encrypted ZIP or RAR files, or password protected Microsoft Office files). Passwords used for decryption must not be sent in the same message as the encrypted content and not to anyone other than the intended recipient.*

- Do not respond to an email, web link or unidentified telephone call requesting your passwords or other information about your account *(Contact the Help Desk to report suspicious requests or to confirm the validity of such requests)*.
- The Firm reserves the right to access, reply, copy, delete, monitor, review, audit and/or disclose use of IT resources or information transmitted to/from these resources to protect and promote compliance with the Firm's business objectives and related policies. Any such access, editing, monitoring, review, audit and/or disclosure activities must be consistent with applicable legal/regulatory requirements.
- Users must respect all copyright and other intellectual property laws. For the Firm's protection as well as for every individual, it is critical to show proper respect for the laws governing copyright, fair use of copyrighted material owned by others, trademarks, and other intellectual property, including the Firm's own copyrights, trademarks, and brands.
- Employees regulated by FINRA (Financial Industry Regulatory Authority), the U.S. Securities and Exchange Commission, the Ontario Securities Commission, or the Financial Conduct Authority (in the UK) are subject to routine monitoring of electronic communications by the compliance team as may be required by relevant securities regulations.
- Users are only permitted to access/utilize Firm's IT resources to which they have been explicitly granted permission. Therefore, unrestricted remote access to end-user workstations shall be limited and strictly controlled.
- User must never introduce security risks into the Firm's IT environment and devices. This includes, but is not limited to:
    - Exploiting vulnerabilities or deficiencies
    - Changing the pre-established security configuration of a Firm IT resource
    - Installing an unauthorized wireless access point onto the corporate network regardless of the access point's configuration
    - Installing/downloading unauthorized, unlicensed, or unapproved software
    - Opening links, files, executables, or macros attached to an email from an unknown, suspicious, or untrustworthy source. Report such type of emails as phishing attempt to Information Security. Hit 'Report Email' add-in available on the right side of outlook ribbon.
        - Contact Information Security/OnePoint/Service Desk for assistance with confirming the validity of emails from unknown, suspicious, or untrustworthy sources.
- When using laptops in public spaces, users are to ensure that their screens cannot be viewed by anyone else.

- When using mobile phones in public spaces, users are to be aware of others overhearing their conversation and to limit any possible disclosure of confidential information.
- Users must not check physical devices (Kroll supplied Laptop/mobile phone/system) as luggage during travel, unless specifically required due to government regulations related to travel in certain countries. In that case, contact the Information Security/Service desk for precautions to be taken prior to travel.
- Users are responsible for the security and secure operation of the Firm's equipment while traveling away from the office.

6.1 Travelling to China and other identified countries.

- When an employee is traveling to countries where there is a risk of the firm's equipment being seized or examined, the user must contact the Information Security Team prior to travel. Sanitized laptops will be provided.
- Users shall not bring corporate laptops or tablets into China when traveling for business or personal reasons. If an employee is traveling to China for work or for personal reasons and wants to work remotely while there, they will need to request a loaner laptop that is approved and configured appropriately.
- Corporate and bring-your-own mobile devices will not be allowed to connect to the Kroll infrastructure while employees are traveling in China. These devices will be disconnected from the Kroll infrastructure and will be re-connected once the user has left China.
- Employees traveling to China can find the new policy and loaner equipment request in OnePoint under the heading "China Access Device Requirements Policy".

7 System Access

All proposed deployments and/or modifications, upgrades or alterations to technology infrastructure must be reviewed and approved by the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) or their delegates. The deployments, modifications, upgrades, and alterations include, but are not limited to:

- Servers or systems (including external or isolated environments that host or otherwise contain and/or access Firm and/or client data)
- Corporate, regional, shared, and local network architecture
- Network security
- Data storage, retention, and deletion schedules

Once approved, IT will follow the change management process and perform the deployment. If the services are being offered by a third-party or deployed outside of the Firm's network, the same process will be followed, and legal approval must also be obtained. Individuals and office locations must not deploy or make modifications without adhering to the above requirements.

8 Information Transmission, Storage and Access

Transmitting, storing, or accessing information in any unapproved manner creates a significant risk to the Firm and its clients. Users are required to utilize only approved applications and processes to transmit, store and access information. Using a file sharing service such as Dropbox, or Google Drive, to create, access, store, upload or download information is a non-secure activity and violates this policy.

Individuals shall not use external third-party file sharing services unless it is documented and approved by the Information Security Team Exceptions may be granted if a client requests the use of an external file sharing service controlled or managed by that client. As soon as practicable, and at the latest when a business engagement ends, all information stored in third-party sites must be removed from the third-party site and transferred into the appropriate Kroll storage to the extent such files are required to be retained in accordance with Kroll Records and Information Management Policy.

Employees shall not use personal, un-authorized file share sites for storage, collaboration, or transfer. This includes sites such as iCloud, Drop Box, Box, OneDrive, or other similar sites. All employees must disclose any legacy storage sites that may have been used prior to any integration. These sites will be disclosed to the Information Security Team during the integration. Please contact the OnePoint/Service Desk if you need assistance setting up secure methods to send or receive information.

9 Remote Access

Remote access is provided to access Firm systems while away from the office. If access is needed to the Firm network or email system, a connection to the VPN network is required. It is the user's responsibility to ensure that no information is compromised as a result of remote access usage. The following actions are prohibited:

- Downloading information to a public computer, or other non-secure device, through remote access.
- Leaving a remote access session unattended, especially in public areas.
- Sharing Firm provided computers, equipment, software, devices, etc. with family members, friends, or others.

10 Third Party Service Providers

Individuals must request an evaluation of any prospective third-party service provider that may have access to Firm systems, information and/or facilities before contracting services. The evaluations are to be performed by the legal, IT. privacy and information security teams. Sharing any data other than that deemed public with an unapproved third-party service provider is expressly prohibited.

11 Internet Usage

The internet shall be used in a responsible, ethical, and lawful manner to facilitate and effect legitimate business purposes. Occasional personal use is permitted and subject to Firm policies. The Firm maintains and operates systems, tools and processes which monitor and restrict internet traffic and the external websites accessed on Firm provided equipment that can be reached when connected to the corporate network. Additionally, these tools have the ability to monitor and restrict the Internet activity performed on Firm-provided equipment while off the corporate network. The Firm maintains audit logs of activities involving network and internet usage. Such logs are used to ensure efficient management of networks and may be used in conducting random audits of employee practices to confirm adherence to Firm policies.

- A monitoring process actively reviews all internet traffic requests in real time and either approves or blocks access to the requested address. Users will receive a notification page if access to a website has been blocked. If the user needs access to a blocked URL/domain, a request ticket should be submitted to OnePoint. Access requests will be reviewed and approved/rejected based on the URL/domain reputation, business justification and duration of access.
- Due to the dynamic nature of the Internet and the constantly evolving threats to the Firm, the monitoring and filtering criteria used to determine if access to a website or category of sites is approved or blocked, may be changed at any time by the Information Security team if a web proxy technology has not updated dynamically.

- Some business groups or user roles may be granted different levels of access or may request additional access based on proven business need.
- All monitoring and filtering are to be performed within the boundaries of local law.
- The Firm network is the only approved method of providing access to the internet from Firm offices. Any other internet service provider used to provide business-related access to the internet from any device connected to the corporate network must be approved by Information Security.
- Users are not permitted to manipulate any monitoring, anti-virus or filtering software or install other software for the purposes of bypassing any monitoring or filtering tools.

Regardless of the level of internet filtering that may be in place, users are responsible for any internet activity conducted on Firm-provided devices, including ensuring they do not visit websites or download files that could be considered questionable or insecure, violate Firm policy or pose a risk to the Firm, even if access to the website was not blocked.

11.1 Convenience Internet Access

In certain locations, the Firm may choose to provide wireless internet access for the convenience of employees, independent contractors, consultants, and visitors in specific areas of Firm offices. This internet access does not connect to the corporate network and is not provided for regular business purposes, but rather for the personal use of users while they are away from their work areas. Use of this internet access should be considered a privilege and all users are expected to exercise good judgment and abide by all relevant Firm policies and on-site guidance when utilizing this internet connectivity.

11.2 Social Networking

Access to social networking websites (e.g., Facebook, Instagram, LinkedIn, etc. is allowed, except where the employee is FINRA-regulated. Access to Twitter and LinkedIn are permitted for FINRA regulated employees only after the employee grants Kroll permission to capture, archive, and routinely review activity on these sites. All use of social networking websites must be conducted in accordance with the social media policy.

12 Suspected Misuse

Employees shall ensure the hardware and software provided by the Firm are utilized in accordance with Firm policies and are protected from theft, physical and other types of damage by taking reasonable precautions. Any individual who suspects incidents of misuse, fraud, loss and/or theft involving Firm IT resources and/or information should immediately report the activity to their supervisor, manager, or local Human Capital business partner.

12.1 Improper Usage

In accordance with the Firm's general acceptable use, there are actions that are deemed as improper and are to be prohibited such as engaging in any activity that is in violation of local, state, federal, international, or applicable law; engaging in personal activities that incur additional costs to the Firm or interfere with employee's work performance and/or productivity; as well as those deemed offensive or harassing. Below are ***improper usage examples*** which are in violation of this Policy, which include, but are not limited to the following sections.

- Engaging in communications that are in violation of Firm policies, including but not limited to transmission of defamatory, obscene, malicious, offensive, or harassing messages, or messages that disclose personal, confidential, and sensitive Firm and client materials or information without authorization and the appropriate level of security.
- Engaging in chat rooms or other forums to release the Firm's confidential, sensitive, or proprietary materials or information, or to purport to represent the Firm or its interests without express authorization.
- Conducting unauthorized business, including but not limited to review, duplication, dissemination, removal, installation, damage or alteration of files, passwords, computer systems/programs, or other property of the Firm, or improper use of information obtained by unauthorized means or the creation of new programs/systems unrelated to Firm business developed using Firm resources at any time.
- Sending Firm proprietary, confidential or sensitive materials or information to anyone other than the intended recipient.
- Forwarding spam, chain letters and other junk emails.
- Downloading, installing, distributing, or using any non-sanctioned or unlicensed software or files on Firm computers or on specified online platforms that could leak or identify Kroll and / or its intellectual property, without the approval of management. Examples include but are not limited to:
    - Software, documents, and other information protected by copyright laws or licensing.
    - Screensavers and non-business-related images.
    - Video or audio files not business related (downloading and streaming).
    - Entertainment-related software or games.
    - Internet games (gambling, simulations, online interactions, etc.)
    - Artificial intelligence (OpenAI and / or similar and related platforms / sites)
    - Chat GPT (or similar platforms / sites.)

- Manipulating or disabling any monitoring, anti-virus or filtering software or installing other software for the purposes of bypassing/disabling any monitoring or filtering tools.
- Viewing, transmitting, or downloading pornographic, sexually explicit, or obscene materials or materials that violate or encourage others to violate the law.
- Utilizing another user's login credentials to gain access to a Firm IT resource or user account.
- Divulging your password to another individual.
- Providing an unauthorized person or entity access to Firm systems or information without prior approval.
- Recording any voice communication, including telephone calls, in violation of the Firm's policies or any local, state, federal or international law.
- Hiding an identity (spoofing) when sending an email so the message appears to have originated from someone or somewhere other than the actual source.
- Hosting or creating any internet service using Firm resources.
- Providing inbound access to any Firm system from the internet or any other external network, software, or application *(Access using Firm computers and VPN, or other secure connection methods provided by the Firm are exempt from this restriction).*
- Providing access to Clients and guests of any Firm office location to any Firm systems other than the guest wireless network.

13 Email Confidentiality Disclaimer

All Firm email communications going externally must include a confidentiality disclaimer statement approved by the legal team.

14 Contacts and Questions

Questions or comments about this Policy should be directed to DL.InformationSecurity@Kroll.com

15 Reference Documentation

- Information Security Policy
- Social Media Policy
- Credential Standard
- ISO27001:2022 (Annex A 5.10 Acceptable Use of information and other associated assets)

16 Revision History

Date	Author	Version	Approver
23 October 2023	Jason Bryant	2.6	David Dunn Aimee Sabolyk

Exhibit A